Health and Human Services Agency
CalOHII California Office of Health Information Integrity

CalPSAB Security Steering Team (SST)

SST CHARTER

(Approved July 30, 2010)

Version	Name	Date	Description
1.0	Kris Young	7/30/2010	Original SST Charter developed and approved by CalOHII Management and Security Steering Team.

CalPSAB Security Steering Team (SST)

1. PURPOSE STATEMENT

The purpose of the CalPSAB Security Steering Team is to provide continuity of knowledge, leadership, oversight and guidance for the Security Committee.

2. MISSION

The SST will provide security policy development oversight through collaboration with stakeholders, policy developers and implementers.

3. SCOPE

The SST will act as the as the central authority for all PSAB security policy and implementation information.

4. PLAN

The list below details the SST Plan for providing security policy development oversight through collaboration with stakeholders, policy developers and implementers:

1. Establish security policy oversight for California HIE efforts
2. Create a monitoring process for security policy implementation to ensure that the intentions of the guidelines are faithfully reproduced
3. Construct a collaborative process for coordination between the SST and all California healthcare entities implementing security policies
4. Establish a process for review and adjustment of security policies based on monitoring feedback
5. Document, and track changes to relevant security standards and guidance that may affect PSAB security policies
6. Establish, direct and support security task group efforts

5. GOALS & OBJECTIVES

1. Establish security policy oversight for California HIE efforts by:
    - Prioritizing security policy issues for adoption and/or revision
    - Ensuring new security guidelines and policies are developed for identified security gaps
    - Coordinating revision of security policies and guidelines

- Establishing a process for review and adjustment of security policies based on monitoring feedback
- Documenting and tracking changes to relevant security standards and guidance that may affect PSAB security policies
- Studying applicability of national security guidelines and standards to California implementations and adapt California implementations to assure alignment with national policy
- Submitting security policy and guideline recommendations to Advisory Board/CalOHII for approval

2. Ensure the intentions of the security guidelines are faithfully reproduced by:
   - Creating a monitoring process for security policy implementation
   - Constructing a collaborative process for coordination between the SST and all California healthcare entities implementing security policies
3. Establish, direct and support security task group efforts by:
   - Providing an open venue for evaluation, analysis and collaboration for development and revision of security policy
   - Provide oversight and coordination of task group efforts
   - Ensure policies and guidelines produced by task groups are in alignment with national standards where applicable (such as federal standards that do not apply to states)
   - Provide rationale, clarification and direction to task groups

6. VOTING PROCEDURES

The following voting procedures will be used for the SST:

1. Voting on issues will be accomplished during meetings or through the use of surveys
2. Voting members must be identified by name and stakeholder representation
3. A quorum of SST members must be present in order to hold a vote
   - A quorum for an SST meeting is 50% or above of the SST

- Two-thirds of SST members constitute a valid vote
- Additionally, a quorum cannot vote if the stakeholder representation includes more than half of a specific stakeholder category
- Results of every vote will be posted with name and stakeholder category

4. A vote passes by general consensus
   - Members may abstain:
     1) If a member abstains, they must state their reason for doing so
5. If voting is evenly split, CalOHII representative and Security Committee Co-Chairs will hold a separate meeting to discuss and make a decision on the split vote
6. If there are dissenting opinion(s), they will be detailed in the recommendation(s) to be forwarded to the Advisory Board

7. MEETING PROCEDURES

The following meeting procedures will be used by the SST:

1. Meeting Dates
   - Will meet monthly or more often as determined by the SST
   - Requirements for posting documents and meeting dates in advance will mirror the CalPSAB (Advisory Board) requirements
2. Meeting Agendas
   - Recap of last meeting
     1) Update of action items from last meeting
   - Updates of activities
     1) Policy Oversight
     2) Standards Monitoring
     3) Task Groups
   - Specific issue discussions

- Call for voting

  1) OHII facilitator or one of the Security Committee Co-chairs will state the issue and the proposed recommended action (policy)

  2) Members will vote yea or nay or abstain

  3) OHII facilitator or one of the Security Committee Co-chairs will state the outcome of the vote as passed, defeated or split

- Update Priority List

- Identify action items from meeting and assignments

8. POLICY RECOMMENDATION PROCESS

Once the SST has voted to adopt a security policy recommendation, the following Policy Recommendation Process will be used by the SST:

1. SST will submit the recommendation to CalOHII Legal for review

2. The finalized recommendation will be inserted into a survey and sent to all Security Committee members for vetting

3. The survey will contain any necessary context and reasoning behind the recommendation and any detailed dissent recorded from the SST approval process

4. All survey comments from Security Committee members will be responded to, if necessary

5. The SST may revise security policy recommendations upon review of survey results and comments

6. The SST will vote on any revisions

7. SST will submit finalized recommendations to the Advisory Board for adoption

9. PARTICIPATION RULES & REQUIREMENTS

9.1. Membership Selection

1. Initial members selected by CalOHII

2. Additional volunteer members will be added at a later date to be determined by the initial SST members

3. New volunteer members will be identified from a future survey and must be recommended by the SST and selected by CalOHII executive staff based on:

    - Past Participation
    - Past Attendance
    - Subject Matter Expertise (SME)
    - Stakeholder Representation

9.2. Participation Requirements

1. SST members must be committed to the CalPSAB principle of safeguarding sensitive health information and the success of HIE in California.

    - Members can be removed on a consensus vote if the SST feels that a member is not committed to safeguarding individual health information or the success of HIE in California.

2. SST Members must maintain a minimum 75% meeting attendance record and 75% participation in surveys

3. If SST members miss three (3) meetings and/or surveys in a row, they will receive a warning

4. If an SST member misses a fourth meeting and/or surveys in a row, they can no longer serve as an SST member. Exceptions will be made on a case-by-case basis.

5. SST members may team up with another individual from their own organization in order to meet these requirements.

    - For example: XYZ employee is on SST. That person may team up with another XYZ employee as long as they communicate with each other on current SST events and remain up-to-date. This “team” would only have one vote even if both members attend a meeting at the same time.

6. SST members must participate on one or more issue/policy

9.3. Reinstatement Process

If a member has been removed from the SST, they may re-apply for membership once they meet the following criteria:

- Attendance of four consecutive meetings and/or surveys

- SST must vote on reinstatement – consideration will be given for past performance and participation
- SME & stakeholder representation will be considered

9.4. Non-Core Security Committee Members

1. Security Committee Membership is open to anyone wanting to join
2. Attendance and participation are not mandatory but is encouraged
3. No voting rights
4. Can apply for core membership (SST) when the SST requests new members
5. SST votes on new members – consideration for past performance and participation
6. Subject matter expertise and stakeholder representation will be considered
7. Must have attended four consecutive meetings or responded to surveys as noted above

9.5. Subject Matter Experts (SMEs)

SMEs will be needed, but not until such time as the SST addresses specific security issues. Depending on the issue, the SST will decide what expertise is needed and when.

10. ROLES & RESPONSIBILITIES

10.1. Security Policy Oversight (SPO)

1. Central clearing house for all PSAB Security Guideline implementation information
2. Monitor policy implementation and receive feedback on existing security policies
3. Evaluate and analyze policy guidelines that are inadequate for implementation
4. Coordinate with the authoring PSAB groups for review and adjustment of inadequate policies.
5. Collaborate with policy implementers
6. Oversee development of new policy guidelines

10.2. Security Standards Monitoring (SSM)

(International, National & State Standards, Guidelines, and Laws & Regulations)

1. Identify, map and track security standards, guidelines and state laws & regulations that affect security policy and implementation of PSAB security policies
2. Identify aligned and non-aligned security policies
3. Keep Security task groups updated on issues related to specific PSAB security groups
4. Keep policy implementers updated on new and revised standards as they relate to PSAB security policies
5. Provide PSAB Security outreach/presentations to other security standards bodies
6. Attend security standards-related Webinars, meetings and conferences and provide update to SST

10.3. Task Groups

1. Participate in task groups
2. Work with other co-chair and OHII staff to identify deliverables
3. Know and understand PSAB related guidelines, as well as other pertinent standards related to the task group you are participating in.
4. Contribute or assist to produce deliverables